SCHWEIZERISCHE EIDGENOSSENSCHAFT
CONFÉDÉRATION SUISSE
SWISS CONFEDERATION

Bescheinigung

Die beiliegenden Akten stimmen überein mit den ursprünglichen Unterlagen der auf den nächsten Seiten bezeichneten, beim unterzeichneten Amt, als Anmeldeamt im Sinne von Art. 10 des Vertrages über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens (PCT), eingegangenen Patentanmeldung.

Attestation

Les documents ci-joints sont conformes aux pièces originales relative à la demande de brevet spécifiée aux pages suivantes, déposées auprès de l'Office soussigné, en tant qu'Office récepteur au sens de l'article 10 du Traité de coopération en matière de brevets (PCT).

Confirmation

It is hereby confirmed that the attached documents are corresponding with the original pages of the international application, as identified on the following pages, filed under Article 10 of the Patent Cooperation Treaty (PCT) at the receiving office named below.

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) or (b)

Bern, 8. Oktober 2002

Eidgenössisches Institut für Geistiges Eigentum
Institut Fédéral de la Propriété Intellectuelle
Swiss Federal Intellectual Property Institute

Patentverfahren
Administration des brevets
Patent Administration

Rolf Hofstetter

VIA TELEFAX (38 Seiten) und BESTÄTIGUNG **CONFIRMATION**

PCT
Anmeldeamtsexemplar

ANTRAG

Der Unterzeichnete beantragt, daß die vorliegende internationale Anmeldung nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens behandelt wird.

Vom Anmeldeamt auszufüllen

PCT/CH 02/00452
Internationales Aktenzeichen

16. Aug. 2002 (16.08.02)
Internationales Anmeldedatum

RO/CH - Internationale Anmeldung PCT
Name des Anmeldeamts und "PCT International Application"

Aktenzeichen des Anmelders oder Anwalts *(falls gewünscht)* *(max. 12 Zeichen)* 153827.1/LE/mb

Feld Nr. I BEZEICHNUNG DER ERFINDUNG

Verfahren und System für GSM-Authentifizierung bei WLAN Roaming

Feld Nr. II ANMELDER ☐ Diese Person ist gleichzeitig Erfinder

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

TOGEWA Holding AG
Worbstrasse 223
3073 Gümligen (Schweiz)

Telefonnr.:

Telefaxnr.:

Fernschreibnr.:

Registrierungsnr. des Anmelders beim Amt:

Staatsangehörigkeit *(Staat)*: CH

Sitz oder Wohnsitz *(Staat)*: CH

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☒ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Feld Nr. III WEITERE ANMELDER UND/ODER (WEITERE) ERFINDER

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

STADELMANN Toni
Bodenacker 69
3065 Bolligen (Schweiz)

Diese Person ist:
☐ nur Anmelder
☒ Anmelder und Erfinder
☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Registrierungsnr. des Anmelders beim Amt:

Staatsangehörigkeit *(Staat)*: CH

Sitz oder Wohnsitz *(Staat)*: CH

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☒ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

☒ Weitere Anmelder und/oder (weitere) Erfinder sind auf einem Fortsetzungsblatt angegeben.

Feld Nr. IV ANWALT ODER GEMEINSAMER VERTRETER; ODER ZUSTELLANSCHRIFT

Die folgende Person wird hiermit bestellt/ist bestellt worden, um für den (die) Anmelder vor den zuständigen internationalen Behörden in folgender Eigenschaft zu handeln als: ☒ Anwalt ☐ gemeinsamer Vertreter

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)*

BOVARD AG
[~~Patentanwälte~~] *
Optingenstrasse 16
3000 Bern 25 (Schweiz)

Telefonnr.: 031/335.20.00

Telefaxnr.: 031/332.81.59

Fernschreibnr.:

Registrierungsnr. des Anwalts beim Amt:

☐ **Zustellanschrift:** Dieses Kästchen ist anzukreuzen, wenn kein Anwalt oder gemeinsamer Vertreter bestellt ist und statt dessen im obigen Feld eine spezielle Zustellanschrift angegeben ist.

* RO

Bestätigungskopie

Blatt Nr. ..2... **PCT/CH 02/00452**

Fortsetzung von Feld Nr. III WEITERE ANMELDER UND/ODER (WEITERE) ERFINDER

Wird keines der folgenden Felder benutzt, so sollte dieses Blatt dem Antrag nicht beigefügt werden.

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

KAUZ Michael
Chemin du Devin 80
1012 Lausanne (Schweiz)

Diese Person ist:
☐ nur Anmelder
☒ Anmelder und Erfinder
☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Registrierungsnr. des Anmelders beim Amt:

Staatsangehörigkeit *(Staat)*: CH

Sitz oder Wohnsitz *(Staat)*: CH

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☒ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

Diese Person ist:
☐ nur Anmelder
☐ Anmelder und Erfinder
☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Registrierungsnr. des Anmelders beim Amt:

Staatsangehörigkeit *(Staat)*:

Sitz oder Wohnsitz *(Staat)*:

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

Diese Person ist:
☐ nur Anmelder
☐ Anmelder und Erfinder
☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Registrierungsnr. des Anmelders beim Amt:

Staatsangehörigkeit *(Staat)*:

Sitz oder Wohnsitz *(Staat)*:

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

Diese Person ist:
☐ nur Anmelder
☐ Anmelder und Erfinder
☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Registrierungsnr. des Anmelders beim Amt:

Staatsangehörigkeit *(Staat)*:

Sitz oder Wohnsitz *(Staat)*:

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

☐ Weitere Anmelder und/oder (weitere) Erfinder sind auf einem zusätzlichen Fortsetzungsblatt angegeben.

Feld Nr. V BESTIMMUNG VON STAATEN *Bitte die entsprechenden Kästchen ankreuzen; wenigstens ein Kästchen muß angekreuzt werden.*

Die folgenden Bestimmungen nach Regel 4.9 Absatz a werden hiermit vorgenommen:

Regionales Patent

☒ **AP** **ARIPO-Patent:** GH Ghana, GM Gambia, KE Kenia, LS Lesotho, MW Malawi, MZ Mosambik, SD Sudan, SL Sierra Leone, SZ Swasiland, TZ Vereinigte Republik Tansania, UG Uganda, ZM Sambia, ZW Simbabwe und jeder weitere Staat, der Vertragsstaat des Harare-Protokolls und des PCT ist *(falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben)* .....

☒ **EA** **Eurasisches Patent:** AM Armenien, AZ Aserbaidschan, BY Belarus, KG Kirgisistan, KZ Kasachstan, MD Republik Moldau, RU Russische Föderation, TJ Tadschikistan, TM Turkmenistan und jeder weitere Staat, der Vertragsstaat des Eurasischen Patentübereinkommens und des PCT ist

☒ **EP** **Europäisches Patent:** AT Österreich, BE Belgien, BG Bulgarien, CH &LI Schweiz und Liechtenstein, CY Zypern, CZ Tschechische Republik, DE Deutschland, DK Dänemark, EE Estland, ES Spanien, FI Finnland, FR Frankreich, GB Vereinigtes Königreich, GR Griechenland, IE Irland, IT Italien, LU Luxemburg, MC Monaco, NL Niederlande, PT Portugal, SE Schweden, SK Slowakei, TR Türkei und jeder weitere Staat, der Vertragsstaat des Europäischen Patentübereinkommens und des PCT ist

☒ **OA** **OAPI-Patent:** BF Burkina Faso, BJ Benin, CF Zentralafrikanische Republik, CG Kongo, CI Côte d'Ivoire, CM Kamerun, GA Gabun, GN Guinea, GQ Äquatorialguinea, GW Guinea-Bissau, ML Mali, MR Mauretanien, NE Niger, SN Senegal, TD Tschad, TG Togo und jeder weitere Staat, der Vertragsstaat der OAPI und des PCT ist *(falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben)* .....

Nationales Patent *(falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben):*

☒ AE Vereinigte Arabische Emirate	☒ GM Gambia	☒ NZ Neuseeland
☒ AG Antigua und Barbuda	☒ HR Kroatien	☒ OM Oman
☒ AL Albanien	☒ HU Ungarn	☒ PH Philippinen
☒ AM Armenien	☒ ID Indonesien	☒ PL Polen
☒ AT Österreich + Gebrauchsmuster (GM)	☒ IL Israel	☒ PT Portugal
☒ AU Australien	☒ IN Indien	☒ RO Rumänien
☒ AZ Aserbaidschan	☒ IS Island	☒ RU Russische Föderation
☒ BA Bosnien-Herzegovina	☒ JP Japan	
☒ BB Barbados	☒ KE Kenia	☒ SD Sudan
☒ BG Bulgarien	☒ KG Kirgisistan	☒ SE Schweden
☒ BR Brasilien	☒ KP Demokratische Volksrepublik	☒ SG Singapur
☒ BY Belarus	Korea	☒ SI Slowenien
☒ BZ Belize	☒ KR Republik Korea	☒ SK Slowakei + GM
☒ CA Kanada	☒ KZ Kasachstan	☒ SL Sierra Leone
☒ CH & LI Schweiz und Liechtenstein	☒ LC Saint Lucia	☒ TJ Tadschikistan
☒ CN China	☒ LK Sri Lanka	☒ TM Turkmenistan
☒ CO Kolumbien	☒ LR Liberia	☒ TN Tunesien
☒ CR Costa Rica	☒ LS Lesotho	☒ TR Türkei
☒ CU Kuba	☒ LT Litauen	☒ TT Trinidad und Tobago
☒ CZ Tschechische Republik + GM	☒ LU Luxemburg	
☒ DE Deutschland + GM	☒ LV Lettland	☒ TZ Vereinigte Republik Tansania
☒ DK Dänemark + GM	☒ MA Marokko	☒ UA Ukraine
☒ DM Dominica	☒ MD Republik Moldau	☒ UG Uganda
☒ DZ Algerien		☒ US Vereinigte Staaten von Amerika
☒ EC Ecuador	☒ MG Madagaskar	
☒ EE Estland + GM	☒ MK Die ehemalige jugoslawische Republik Mazedonien	☒ UZ Usbekistan
☒ ES Spanien		☒ VN Vietnam
☒ FI Finnland + GM	☒ MN Mongolei	☒ YU Jugoslawien
☒ GB Vereinigtes Königreich	☒ MW Malawi	☒ ZA Südafrika
☒ GD Grenada	☒ MX Mexiko	☒ ZM Sambia
☒ GE Georgien	☒ MZ Mosambik	☒ ZW Simbabwe
☒ GH Ghana	☒ NO Norwegen	

Kästchen für die Bestimmung von Staaten, die dem PCT nach der Veröffentlichung dieses Formblatts beigetreten sind.

☒ VC St. Vincent und die Grenadinen	☐	☐

Erklärung bzgl. vorsorglicher Bestimmungen: Zusätzlich zu den oben genannten Bestimmungen nimmt der Anmelder nach Regel 4.9 Absatz b auch alle anderen nach dem PCT zulässigen Bestimmungen vor mit Ausnahme der im Zusatzfeld genannten Bestimmungen, die von dieser Erklärung ausgenommen sind. Der Anmelder erklärt, daß diese zusätzlichen Bestimmungen unter dem Vorbehalt einer Bestätigung stehen und jede zusätzliche Bestimmung, die vor Ablauf von 15 Monaten ab dem Prioritätsdatum nicht bestätigt wurde, nach Ablauf dieser Frist als vom Anmelder zurückgenommen gilt. *(Die Bestätigung (einschließlich der Gebühren) muß beim Anmeldeamt innerhalb der Frist von 15 Monaten eingehen.)*

Feld Nr. VI PRIORITÄTSANSPRUCH

Die Priorität der folgenden früheren Anmeldung(en) wird hiermit in Anspruch genommen:

Anmeldedatum der früheren Anmeldung *(Tag/Monat/Jahr)*	Aktenzeichen der früheren Anmeldung	Ist die frühere Anmeldung eine:		
		nationale Anmeldung: Staat oder Mitglied der WTO	regionale Anmeldung:* regionales Amt	internationale Anmeldung: Anmeldeamt
Zeile (1) --	--	--		
Zeile (2)				
Zeile (3)				
Zeile (4)				
Zeile (5)				

☐ Weitere Prioritätsansprüche sind im Zusatzfeld angegeben.

Das Anmeldeamt wird ersucht, eine beglaubigte Abschrift der oben bezeichneten früheren Anmeldung(en) zu erstellen und dem internationalen Büro zu übermitteln *(nur falls die frühere Anmeldung(en) bei dem Amt eingereicht worden ist (sind), das für die Zwecke dieser internationalen Anmeldung Anmeldeamt ist)*:

☐ sämtliche Zeilen ☐ Zeile (1) ☐ Zeile (2) ☐ Zeile (3) ☐ Zeile (4) ☐ Zeile (5) ☐ weitere, siehe Zusatzfeld

** Falls es sich bei der früheren Anmeldung um eine ARIPO-Anmeldung handelt, geben Sie mindestens einen Staat an, der Mitgliedstaat der Pariser Verbandsübereinkunft zum Schutz des gewerblichen Eigentums oder Mitglied der Welthandelsorganisation ist und für den oder das die frühere Anmeldung eingereicht wurde:* .....

Feld Nr. VII INTERNATIONALE RECHERCHENBEHÖRDE

Wahl der internationalen Recherchenbehörde (ISA) *(falls zwei oder mehr als zwei internationale Recherchenbehörden für die Ausführung der internationalen Recherche zuständig sind, geben Sie die von Ihnen gewählte Behörde an; der Zweibuchstaben-Code kann benutzt werden)*:

ISA / .....

Antrag auf Nutzung der Ergebnisse einer früheren Recherche; Bezugnahme auf diese frühere Recherche *(falls eine frühere Recherche bei der internationalen Recherchenbehörde beantragt oder von ihr durchgeführt worden ist)*:

Datum *(Tag/Monat/Jahr)* Aktenzeichen Staat *(oder regionales Amt)*

Feld Nr. VIII ERKLÄRUNGEN

Die Felder Nr. VIII (i) bis (v) enthalten die folgenden Erklärungen *(Kreuzen Sie unten die entsprechenden Kästchen an und geben Sie in der rechten Spalte für jede Erklärung deren Anzahl an)* :		Anzahl der Erklärungen
☐ Feld Nr. VIII (i)	Erklärung hinsichtlich der Identität des Erfinders :	
☐ Feld Nr. VIII (ii)	Erklärung hinsichtlich der Berechtigung des Anmelders, zum Zeitpunkt des internationalen Anmeldedatums, ein Patent zu beantragen und zu erhalten :	
☐ Feld Nr. VIII (iii)	Erklärung hinsichtlich der Berechtigung des Anmelders, zum Zeitpunkt des internationalen Anmeldedatums, die Priorität einer früheren Anmeldung zu beanspruchen :	
☐ Feld Nr. VIII (iv)	Erfindererklärung (nur im Hinblick auf die Bestimmung der Vereinigten Staaten von Amerika) :	1 (folgt)
☐ Feld Nr. VIII (v)	Erklärung hinsichtlich unschädlicher Offenbarungen oder Ausnahmen von der Neuheitsschädlichkeit :	

PCT/CH 02 / 00452

Blatt Nr. ...6...

Feld Nr. IX KONTROLLISTE; EINREICHUNGSSPRACHE

Diese internationale Anmeldung enthält:

(a) die folgende Anzahl an Blättern Papier:

Antrag (inklusive Erklärungsblätter)	:	6
Beschreibung (ohne Sequenzprotokollteil)	:	21
Ansprüche	:	5
Zusammenfassung	:	1
Zeichnungen	:	5
Teilanzahl	:	38
Sequenzprotokollteil der Beschreibung *(Anzahl der Blätter, soweit auf Papier eingereicht wird, unabhängig davon, ob zusätzlich auch in computerlesbarer Form eingereicht wird)*	:	
Gesamtanzahl	:	38

(b) Sequenzprotokollteil der Beschreibung in computerlesbarer Form eingereicht

(i) ☐ ausschließlich in dieser Form (nach Abschnitt 801(a)(i))

(ii) ☐ zusätzlich zur Einreichung auf Papier (nach Abschnitt 801(a)(ii))

Art und Anzahl der Datenträger (Diskette, CD-ROM, CD-R oder sonstige), auf denen der Sequenzprotokollteil enthalten ist *(zusätzlich eingereichte Kopien unter Punkt 9(ii) in der rechten Spalte angeben)*:

.....

Dieser internationalen Anmeldung liegen die folgenden Unterlagen bei *(kreuzen Sie die entsprechenden Kästchen an und geben Sie in der rechten Spalte jeweils die Anzahl der beiliegenden Exemplare an)*

		Anzahl
1. ☒ Blatt für die Gebührenberechnung	:	1
2. ☐ Original einer gesonderten Vollmacht folgt	:	
3. ☐ Original einer allgemeinen Vollmacht	:	
4. ☐ Kopie der allgemeinen Vollmacht; Aktenzeichen (falls vorhanden):	:	
5. ☐ Begründung für das Fehlen einer Unterschrift	:	
6. ☐ Prioritätsbeleg(e), in Feld Nr. VI durch folgende Zeilennummer(n) gekennzeichnet:	:	
7. ☐ Übersetzung der internationalen Anmeldung in die folgende Sprache:	:	
8. ☐ Gesonderte Angaben zu hinterlegten Mikroorganismen oder anderem biologischen Material	:	
9. ☐ Sequenzprotokoll in computerlesbarer Form (geben Sie zusätzlich die Art und Anzahl der beiliegenden Datenträger an (Diskette, CD-ROM, CD-R oder sonstige))		
(i) ☐ Kopie ausschließlich für die Zwecke der internationalen Recherche nach Regel 13*ter* (und nicht als Teil der internationalen Anmeldung)	:	
(ii) ☐ *(nur falls Feld (b)(i) oder (b)(ii) in der linken Spalte angekreuzt wurde)* zusätzliche Kopien einschließlich, soweit zutreffend, einer Kopie für die Zwecke der internationalen Recherche nach Regel 13*ter*	:	
(iii) ☐ zusammen mit entsprechender Erklärung, daß die Kopie(n) mit dem in der linken Spalte aufgeführten Sequenzprotokollteil identisch ist (sind)	:	
10. ☐ Sonstige *(einzeln aufführen)*:	:	

Abbildung der Zeichnungen, die mit der Zusammenfassung veröffentlicht werden soll (Nr.): 1

Sprache, in der die internationale Anmeldung eingereicht wird: Deutsch

Feld Nr. X UNTERSCHRIFT DES ANMELDERS, DES ANWALTS ODER DES GEMEINSAMEN VERTRETERS

Der Name jeder unterzeichnenden Person ist neben der Unterschrift zu wiederholen, und es ist anzugeben, sofern sich dies nicht eindeutig aus dem Antrag ergibt, in welcher Eigenschaft die Person unterzeichnet.

ROVARD AG

J. Aebischer

Vom Anmeldeamt auszufüllen

1. Datum des tatsächlichen Eingangs dieser internationalen Anmeldung: 16. Aug. 2002 (16.08.02)

2. Zeichnungen:
☐ eingegangen:
☐ nicht eingegangen:

3. Geändertes Eingangsdatum aufgrund nachträglich, jedoch fristgerecht eingegangener Unterlagen oder Zeichnungen zur Vervollständigung dieser internationalen Anmeldung:

4. Datum des fristgerechten Eingangs der angeforderten Richtigstellungen nach Artikel 11(2) PCT:

5. Internationale Recherchenbehörde *(falls zwei oder mehr zuständig sind)*: ISA /

6. ☐ Übermittlung des Recherchenexemplars bis zur Zahlung der Recherchengebühr aufgeschoben

Vom Internationalen Büro auszufüllen

Datum des Eingangs des Aktenexemplars beim Internationalen Büro:

Verfahren und System für GSM-Authentifizierung bei WLAN Roaming

Die vorliegende Erfindung betrifft ein Verfahren und System für automatisches Roaming zwischen unterschiedlichen WLANs und/oder GSM/GPRS/UMTS-Netzwerken, bei welchem zur Authentifizierung ein mobiler IP-Node über eine drahtlose Schnittstelle innerhalb einer Basic Service Area eines WLANs bei einem Access Server Zugriff auf das WLAN fordert, wobei die Basic Service Area des WLAN ein oder mehrere dem Access Server zugeordnete Access Points umfasst, und der mobile IP-Node mittels einer auf einer SIM-Karte des mobilen IP-Nodes gespeicherte IMSI authentifiziert wird. Insbesondere betrifft die Erfindung ein Verfahren für mobile Nodes in heterogenen WLANS.

In den letzten Jahren ist weltweit die Zahl der Internetbenutzer und damit der dort angebotenen Information exponentiell gestiegen. Obwohl jedoch das Internet weltweit Zugang zu Informationen bietet, hat der Benutzer normalerweise keinen Zugang dazu, bis er nicht an einem bestimmten Netzzugang, wie z.B. im Büro, in der Schule, an der Universität oder zu Hause, angekommen ist. Das wachsende Angebot an IP-fähigen mobilen Geräten, wie z.B. PDAs, Mobilfunktelefonen und Laptops, beginnt unsere Vorstellung vom Internet zu verändern. Ein analoger Übergang von fixen Nodes in Netzwerken zu flexibleren Anforderungen durch erhöhte Mobilität hat eben erst begonnen. In der Mobilfunktelefonie z.B. zeigt sich diese Tendenz u.a. auch an neuen Standards wie WAP, GPRS oder UMTS. Um den Unterschied zwischen der momentanen Realität und den IP-Verbindungsmöglichkeiten der Zukunft zu verstehen, kann man sich als Vergleich die Entwicklung der Telefonie Richtung Mobilität in den letzten zwanzig Jahren vors Auge rufen. Der Bedarf im privaten wie auch im geschäftlichen Bereich nach weltweitem unabhängigem drahtlosen Zugriff auf LANs (z.B. in Flughäfen, Konferenzzentren, Messegeländen, Städten, etc., etc.) mit Laptops, PDAs etc. ist riesig. Die WLANs, basierend z.B. auf IP, bieten heute jedoch den Service nicht, wie er z.B. mit GSM/GPRS erzeugt wird, der ein freies Roaming der Benutzer erlauben würde. Diese Dienste müssten neben Sicherheitsmechanismen wie im GSM/GPRS ebenfalls Möglichkeiten zur Service Autorisierung und zum Billing, d.h. Verrechnen der beanspruchten Leistung etc., umfassen. Auf der anderen Seite wird ein solcher

Dienst auch nicht von bestehenden GSM/GPRS Betreibern angeboten. Es ist aber nicht nur das Roaming zwischen verschiedenen WLANs wichtig. Durch den grossen Wachstum bei der Informationstechnologie mit WLANs (mit Zugriff auf Internet etc.) und dem ebenfalls grossen Wachstum in der Mobilfunktelefonie ist es sinnvoll, diese beiden Welten zu verknüpft. Erst die Verknüpfung der beiden Welten macht bei wireless LANs ein einfaches und automatisches Roaming möglich, wie es der Benutzer von der Mobilfunktechnologie gewohnt ist. Somit besteht der Bedarf nach Anbietern, die zwischen unterschiedlichen WLAN-Dienstanbietern und zwischen WLAN-Dienstanbietern und GSM/GPRS-Dienstanbietern ein standartübergreifendes Roaming ermöglichen.

Computernetze oder Local Area Networks (LAN) bestehen üblicherweise aus sog. Nodes, welche verbunden sind über physikalische Medien, wie z.B. Koaxialkabel, Twisted Pair oder optische Glasfaserkabel. Diese LANs werden auch als wired LANs (verdrahtete Festnetze) bezeichnet. In den letzten Jahren sind auch drahtlose LANs, sog. wireless LANs, immer populärer geworden (z.B. durch Entwicklungen wie das AirPort-System der Apple Computer, Inc. etc.). Wireless LANs sind speziell geeignet, um mobile Einheiten (Nodes), wie z.B. Laptops, Notebooks, PDAs (Personal Digital Assistant) oder Mobilfunkgeräte, insbesondere Mobilfunktelefone, mit einer entsprechenden Schnittstelle in ein lokales Computernetzwerk einzubinden. Die mobilen Nodes besitzen einen Adapter, welcher einen Sender/Empfänger sowie eine Kontrollkarte umfasst (wie z.B. Infrarot(IR)-Adapter oder einen Tieffrequenzradiowellen-Adapter). Der Vorteil von solchen mobilen Nodes ist, dass sie innerhalb der Reichweite des wireless LANs frei bewegt werden können. Die mobilen Nodes kommunizieren entweder direkt miteinander (Peer-to-Peer wireless LAN) oder schicken ihr Signal an eine Basisstation, welche das Signal verstärkt und/oder weiterleitet. Die Basisstationen können ebenfalls Bridgefunktionen umfassen. Über solche Basisstationen mit Bridge-Funktionen, sog. Access Points (AP), können die mobilen Nodes des drahtlosen LAN auf ein wired LAN zugreifen. Typische Netzwerkfunktionen eines Access Points umfassen das Übertragen von Meldungen von einem mobilen Node zu einem anderen, das Senden von Meldungen vom wired LAN zu einem mobilen Node und das Übertragen von Meldungen eines mobilen Nodes auf das wired LAN.

Die physikalische Reichweite eines AP wird Basic Service Area (BSA) genannt. Befindet sich ein mobiler Node innerhalb der BSA eines AP, kann er mit diesem AP kommunizieren, falls der AP ebenfalls innerhalb der Signal-Reichweite (Dynamic Service Area (DSA)) des mobilen Nodes liegt. Mehrere APs sind i.N. einem Access Server zugeordnet, der u.a. die Autorisierung der mobilen Nodes mittels einer Benutzerdatabank überwacht und verwaltet. Die gesamte Fläche, die von den APs eines Access Servers abgedeckt wird, wird als sog. Hot Spot bezeichnet. Mobile Nodes besitzen typischerweise eine Signalstärke von 100 mWatt bis zu einem Watt. Um das wireless LAN mit dem wired LAN zu verbinden, ist es für den AP wichtig zu bestimmen, ob eine bestimmte Meldung (information frame) auf dem Netz für einen Node bestimmt ist, der innerhalb des wired LAN oder innerhalb des wireless LAN liegt, und diese Information, falls notwendig, an den entsprechenden Node weiterzuleiten. Für diesen Zweck besitzen APs sog. Bridge-Funktionen, z.B. entsprechend dem Standard IEEE Std 802.1D-1990 "Media Access Control Bridge" (31-74 ff). Bei solchen Bridgefunktionen wird ein neuer mobiler Node im wireless LAN typischerweise in einer FDB (Filtering Database) des AP registriert, in dessen Reichweite der Node liegt. Bei jedem Information-Frame auf dem LAN vergleicht der AP die Zieladresse mit den Adressen (MAC-Adressen (Media Access Control Addresses)), welche er im FDB abgespeichert hat und sendet, verwirft oder überträgt den Frame auf das wired LAN bzw. auf das wireless LAN.

Bei mobiler Netzwerkbenutzung sollte ein bestehender IP-Zugriff von Applikationen auf dem mobilen Node nicht unterbrochen werden, wenn der Benutzer seinen Standort im Netzwerk ändert. Im Gegenteil sollten alle Verbindungs- und Schnittstellenänderungen z.B. bei einem Wechsel in unterschiedlichen Hot Spots, insbesondere unterschiedlichen Netzwerken (Ethernet, Mobilfunknetz, WLAN, Bluetooth etc.) automatisch und nicht interaktiv geschehen können, so dass der Benutzer davon nicht einmal Kenntnis zu haben braucht. Dies gilt auch z.B. während der Benutzung von Real-Time Applikationen. Wirkliches mobiles IP-Computing weist viele Vorteile basierend auf einem jederzeitigen stabilen Zugang zum Internet auf. Mit einem solchen Zugang lässt sich die Arbeit frei und unabhängig vom Schreibtisch gestalten. Die Anforderungen an mobile Nodes in Netzwerken unterscheidet sich aber von der eingangs erwähnten Entwicklung in der Mobilfunktechnik auf

verschiedene Arten. Die Endpunkte im Mobilfunk sind gewöhnlich Menschen. Bei mobilen Nodes können aber Computerapplikationen Interaktionen zwischen anderen Netzteilnehmern ohne jegliches menschliches Zutun oder Eingreifen ausführen. Beispiele dazu finden sich in Flugzeugen, Schiffen und Automobilen zu Genüge. So kann insbesondere mobiles Computing mit Internet Zugriff zusammen mit anderen Applikationen wie z.B. in Kombination mit Positionsbestimmungsgeräten, wie dem satellitenbasierenden GPS (Global Positioning System) sinnvoll sein.

Eines der Probleme beim mobilen Netzwerkzugriff via Internet Protokoll (IP) ist, dass das IP-Protokoll, welches dazu benutzt wird, die Datenpakete von der Quelladresse (Source Address) zur Zieladresse (Destination Address) im Netz zu routen, sog. IP-Adressen (IP: Internet Protocol) benutzt. Diese Adressen sind einem festen Standort im Netzwerk zugeordnet, ähnlich wie die Telefonnummern des Festnetzes einer physikalischen Dose zugeordnet sind. Wenn die Zieladresse der Datenpakete ein mobiler Node ist, bedeutet das, dass bei jedem Netzwerkstandortwechsel eine neue IP-Netzwerkadresse zugeordnet werden muss, was den transparenten, mobilen Zugriff verunmöglicht. Diese Probleme wurden durch den Mobile IP Standart (IETF RFC 2002, Okt. 1996) der Internet Engineering Task Force (IETF) gelöst, indem das Mobile IP dem mobilen Node erlaubt, zwei IP-Adressen zu benutzen. Die eine davon ist die normale, statische IP-Adresse (Home-Adresse), die den Ort des Heimnetzes angibt, während die zweite eine dynamische IP Care-Of-Adresse ist, die den aktuellen Standort des mobilen Nodes im Netz bezeichnet. Die Zuordnung der beiden Adressen erlaubt es, die IP-Datenpakete an die richtige, momentane Adresse des mobilen Nodes umzuleiten.

Eine der häufigst verwendeten Protokolle zur Authentifizierung eines Benutzers in einem wireless LAN ist das opensource Protokoll IEEE 802.1x (in der aktuellen Version 802.11) der Institute of Electrical and Electronics Engineers Standards Association. Die IEEE 802.1x Authentifizierung erlaubt den authentifizierten Zugriff auf IEEE 802 Medien, wie z.B. Ethernet, Tokenring und/oder 802.11 wireless LAN. Das 802.11 Protokoll erzeugt für wireless LAN, d.h. für drahtlose, lokale Netzwerke, eine 1 Mbps, 2 Mbps oder 11 Mbps Übertragung im 2.4 GHz Band, wobei entweder FHSS (Frequency Hopping

Spread Spectrum) oder DSSS (Direct Sequence Spread Spectrum) benutzt wird. 802.1x unterstützt zur Authentifizierung EAP (Extensible Authentication Protocol) und TLS (Wireless Transport Layer Security). 802.11 unterstützt ebenfalls RADIUS. Obwohl die RADIUS-Unterstützung bei 802.1x optional ist, ist zu erwarten, dass die meisten 802.1x Authenticators RADIUS unterstützen werden. Das IEEE 802.1x Protokoll ist ein sog. Port-basierendes Authentifizierungsprotokoll. Es kann in jeder Umgebung verwendet werden, in welcher ein Port, d.h. eine Interface eines Gerätes, bestimmt werden kann. Bei der Authentifizierung basierend auf 802.1x können drei Einheiten unterschieden werden. Das Gerät des Benutzers (Supplicant/Client), den Authenticator und den Authentifikationsserver. Der Authenticator ist dafür zuständig, den Supplicant zu authentifizieren. Authenticator und Supplicant sind beispielsweise über ein Point-to-Point LAN Segment oder eine 802.11 wireless Link verbunden. Authenticator und Supplicant besitzen einen definierten Port, eine sog. Port Access Entity (PAE), die einen physikalischen oder virtuellen 802.1x Port definiert. Der Authentifikationsserver erzeugt die vom Authenticator benötigten Authentifikationsdienste. So verifiziert er die vom Supplicant gelieferten Berechtigungsdaten bezüglich der beanspruchten Identität.

Die Authentifikationsserver basieren meistens auf RADIUS (Remote Authentication Dial-In User Service) der IETF (Internet Engineering Task Force). Die Benutzung des RADIUS Authentifizierungsprotokoll und Accountsystems ist weit verbreitet bei Netzwerkeinheiten, wie z.B. Router, Modemserver, Switch etc. und wird von den meisten Internet Service Providern (ISP) benutzt. Wählt sich ein Benutzer bei einem ISP ein, muss er normalerweise einen Benutzernamen und ein Passwort eingeben. Der RADIUS-Server überprüft diese Information und autorisiert den Benutzer zum ISP-System. Der Grund für die Verbreitung von RADIUS liegt u.a. darin, dass Netzwerkeinheiten im allgemeinen nicht mit einer sehr grossen Anzahl Netzbenutzer mit jeweils unterschiedlicher Authentifizierungsinformation umgehen können, da dies z.B. die Speicherkapazität der einzelnen Netzwerkeinheiten übersteigen würde. RADIUS erlaubt die zentrale Verwaltung von einer Vielzahl von Netzwerkbenutzern (Hinzufügen, Löschen von Benutzern etc.). So ist das z.B. bei ISP (Internet Service Providern) eine notwendige Voraussetzung für ihren Dienst, da ihre Benutzeranzahl häufig mehrere tausend

bis mehrere zehntausend Benutzer umfasst. RADIUS erzeugt weiter einen bestimmten permanenten Schutz vor Hackern. Die Remoteauthentifizierung von RADIUS basierend auf TACACS+ (Terminal Access Controller Access Control System+) und LDAP (Lightweight Directory Access Protocol) ist gegen Hacker relativ sicher. Viele andere Remote Authentifizierungsprotokolle haben dagegen nur einen zeitweisen, ungenügenden oder gar keinen Schutz vor Hackerangriffen. Ein andere Vorteil ist, dass RADIUS zurzeit der de-facto Standard für Remote Authentifizierung ist, womit RADIUS auch von fast allen Systemen unterstützt wird, was bei anderen Protokollen nicht der Fall ist.

Das oben erwähnte Extensible Authentication Protocol (EAP) ist eigentlich eine Erweiterung zum PPP (Point-to-Point Protocol) und ist definiert durch das Request for Comments (RFC) 2284 *PPP Extensible Authentification Protocol (EAP)* der IETF. Mittels PPP lässt sich ein Computer z.B. an den Server eines ISP anbinden. PPP arbeitet im Data Link Layer des OSI Model und schickt die TCP/IP-Packete des Computers an den Server des ISP, der das Interface zum Internet bildet. Im Gegensatz zum älteren SLIP Protokoll (Serial Line Internet Protocol) arbeitet PPP stabiler und besitzt Fehlerkorrekturen. Das Extensible Authentication Protocol ist ein Protokoll auf einem sehr allgemeinen Level, das die verschiedensten Authentifizierungsverfahren unterstützt, wie z.B. Token Cards, Kerberos des Massachusetts Institute of Technology (MIT), Streichlisten-Passwörter, Zertifikate, Public Key Authentication und Smartcards oder sog. Integrated Circuit Cards (ICC). IEEE 802.1x definiert die Spezifikationen, wie EAP in die LAN-Frames intergriert sein müssen. Bei Kommunikation in drahtlosen Netzwerken mittels EAP verlangt ein Benutzer über die drahtlose Kommunikation bei einen Access Point (AP), d.h. eines Verbindungs-HUP für den Remote Access Client oder Supplicant zum WLAN, Zugriff auf das wireless LAN. Der AP fordert darauf vom Supplicant die Identifikation des Benutzers und übermittelt die Identifikation an den oben genannten Authentifikationsserver, der z.B. auf RADIUS basiert. Der Authentifikationsserver lässt den Access Point die Identifikation des Benutzers rücküberprüfen. Der AP holt sich diese Authentifizierungsdaten vom Supplicant und übermittelt diese an den Authentifikationsserver, der die Authentifizierung beendet.

Bei EAP erzeugt ein beliebiges Authentifizierungsverfahren eine Remote Access Verbindung. Das genaue Authentifikationsschema wird jeweils zwischen dem Supplicant und dem Authenticator (d.h. dem Remote Access Server, dem Internet Authentification Service (IAS) Server bzw. bei WLAN dem Access Point) festgelegt. Wie oben erwähnt, unterstützt EAP dabei viele unterschiedliche Authentifikationsschemata, wie z.B. generische Token Card, MD5-Challenge, Transport Level Security (TLS) für Smartcards, S/Key und mögliche zukünftige Authentifizierungstechnologien. EAP erlaubt eine von der Anzahl nicht beschränkte Frage-Antwort-Kommunikation zwischen Supplicant und Authenticator, wobei der Authenticator bzw. der Authentifikationsserver spezifische Authentifizierungsinformation verlangt und der Supplicant, d.h. der Remote Access Client antwortet. Beispielsweise kann der Authentifikationsserver über den Authenticator bei den sog. Security Token Cards einzeln zuerst einen Benutzernamen, dann eine PIN (Personal Identity Number) und schlussendlich einen Token Card Value vom Supplicant verlangen. Bei jedem Frage-Antwort-Durchgang wird dabei ein weiterer Authentifizierungslevel durchgeführt. Werden alle Authentifizierungslevel erfolgreich beantwortet, ist der Supplicant authentifiziert. Ein spezifisches EAP Authentifikationsschema wird als EAP-Typ bezeichnet. Beide Seiten, d.h. Supplicant und Authenticator müssen den gleichen EAP-Typ unterstützen, damit die Authentifizierung durchgeführt werden kann. Wie erwähnt, wird dies zu Beginn zwischen Supplicant und Authenticator festgelegt. Authentifikationsserver basierend auf RADIUS unterstützen im Normalfall EAP, was die Möglichkeit gibt, EAP-Meldungen an einen RADIUS-Server zu schicken.

Im Stand der Technik sind ebenfalls EAP-basierende Verfahren zur Authentifizierung eines Benutzers und zur Vergabe von Sessions Keys an den Benutzer mittels des GSM Subscriber Identity Modul (SIM) bekannt. Die GSM Authentifizierung basiert auf einem Frage-Antwort-Verfahren, einem sog. Challenge-Response Verfahren. Dem Authentifikationsalgorithmus der SIM-Karte wird als Challenge (Frage) eine 128-bit Zufallszahl (üblicherweise bezeichnet als RAND) gegeben. Auf der SIM-Karte läuft dann ein für den jeweiligen Operator spezifischen, vertraulichen Algorithmus, der als Input die Zufallszahl RAND und einen geheimen, auf der SIM-Karte gespeicherten

Schlüssel Ki erhält und daraus eine 32-bit Antwort (SRES) und ein 64-bit Schlüssel Kc generiert. Kc ist zur Verschlüsslung des Datentransfers über drahtlose Schnittstellen gedacht (GSM Technical Specification GSM 03.20 (ETS 300 534): "Digital cellular telecommunication system (Phase 2); Security related network functions", European Telecommunications Standards Institute, August 1997). Bei der EAP/SIM Authentifizierung werden mehrere RAND Challenge zum Generieren von mehreren 64-bit Kc Schlüsseln verwendet. Diese Kc-Schlüssel werden zu einem längeren Session Key kombiniert. Mit EAP/SIM erweitert das normale GSM Authentifizierungsverfahren, indem die RAND-Challenges zusätzlich einen Message Authentification Code (MAC) besitzen, um gegenseitige Authentifizierung zu erzeugen. Um die GSM-Authentifizierung durchzuführen, sollte der Authentifikationsserver ein Interface zum GSM-Netzwerk besitzen. Der Authentifikationsserver arbeitet folglich als ein Gateway zwischen Internet Authentification Service (IAS) Server Netzwerk und der GSM Authentifikationsinfrastruktur. Zu Beginn der EAP/SIM Authentifizierung verlangt der Authentifikationsserver mit einem ersten EAP-Request durch den Authenticator vom Supplicant u.a. die International Mobile Subscriber Identity (IMSI) des Benutzers. Mit der IMSI erhält der Authentifikationsserver auf Anfrage vom Authentifikationszenter (AuC) des entsprechenden Mobilfunknetz-Dienstanbieter, üblicherweise im GSM-Netzwerk als Home Location Register (HLR) bzw. Visitor Location Register (VLR) bezeichnet, n GSM Triplets. Von den Triplets erhält der Authentifikationsserver ein Message Authentification Code für n*RAND und eine Lebensdauer für den Schlüssel (zusammen MAC_RAND) sowie einen Session Schlüssel. Mit diesen kann der Authentifikationsserver die GSM-Authentifizierung auf der SIM-Karte des Supplicant bzw. des Benutzers durchführen. Da RAND zusammen mit dem Message Authentification Code MAC_RAND an den Supplicant gegeben wird, wird es für den Supplicant möglich zu überprüfen, ob die RANDs neu sind und durch das GSM-Netzwerk generiert wurden.

Der Stand der Technik hat jedoch verschiedenste Nachteile. Zwar ist es möglich, z.B. mit einer EAP-SIM Authentifizierung die Authentifizierungsverfahren von den GSM-Netzwerken in der wireless LAN-Technologie zur Authentifizierung von Supplicants bzw. Remote Access Clients zu verwenden, vorausgesetzt der Benutzer besitzt eine IMSI bei einem GSM

Dienstanbieter. Ebenso ist es prinzipiell möglich, mittels z.B. Mobile IP der IETF (Internet Engineering Task Force) Datenströme zum entsprechenden bei einem Access Servers über einen Access Point angemeldeten mobilen Remote Access Client umzuleiten (routen). Damit sind jedoch bei weitem nicht alle Probleme der mobilen Netzwerkbenutzung gelöst, welche ein wirklich freies Roaming des Benutzers erlauben würden. Eines der Probleme ist, dass im IP-Netzwerk die im GSM Standart benötigten Voraussetzungen bezüglich Sicherheit, Billing und Service Autorisierung nicht mehr gegeben ist. Dies hängt intrinsisch mit der offenen Architektur des IP-Protokolles zusammen. D.h., viele Informationen fehlen im IP-Standard, die zur vollen Kompatibilität mit den GSM-Netzwerken unbedingt benötigt werden. Zudem liefert ein Access Server beruhend z.B. auf RADIUS ein einzelner Datenstrom. Dieser kann nicht ohne weiteres auf den mehrteiligen Datenstrom des GSM-Standards gemappt werden. Ein anderer Nachteil des Standes der Technik ist, dass wireless LAN heute auf individuellen Hot Spots (d.h. der Basic Service Area der Access Points eines Access Servers) beruhen, die von unterschiedlichen Software- und Hardwareentwicklern der ganzen Welt angeboten werden. Dies erschwert die Zusammenführung beider Welten, da solche Gateway-Funktionen jeweils an die spezifische Lösung angepasst werden müssen. Die technischen Spezifikationen zum GSM Authentifikations-Interface könne in MAP (Mobile Application Part) GSM 09.02 Phase 1 Version 3.10.0 gefunden werden.

Es ist eine Aufgabe dieser Erfindung, ein neues Verfahren für mobile Nodes in heterogenen WLANs vorzuschlagen. Insbesondere soll einem Benutzer ermöglicht werden, problemlos sich zwischen verschiedenen Hot Spots zu bewegen (roaming), ohne dass er sich um Anmeldung, Billing, Service Autorisation etc. bei den verschiedenen WLAN-Dienstanbietern bemühen müsste, d.h. den gleichen Komfort geniesst, wie er es von der Mobilfunktechnologie , wie z.B. GSM, gewohnt ist. Die Erfindung soll die benötigten Komponenten für Billing, Service Autorisierung und Sicherheit für den Benutzer und Serviceanbieter in WLANs sicherstellen.

Gemäss der vorliegenden Erfindung werden diese Ziele insbesondere durch die Elemente der unabhängigen Ansprüche erreicht. Weitere vor-

teilhafte Ausführungsformen gehen ausserdem aus den abhängigen Ansprüchen und der Beschreibung hervor.

Insbesondere werden diese Ziele durch die Erfindung dadurch erreicht, dass zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken zur Authentifizierung ein mobiler IP-Node über eine drahtlose Schnittstelle innerhalb einer Basic Service Area eines WLANs bei einem Access Point Zugriff auf das WLAN fordert, welche Basic Service Area des WLAN ein oder mehrere einem Access Server zugeordnete Access Points umfasst, dass der mobile IP-Node auf einen Request des Access Servers eine auf einer SIM-Karte des mobilen IP-Nodes gespeicherte IMSI an den Access Server übermittelt und dass mittels eines SIM-RADIUS-Moduls die IMSI des IP-Nodes gespeichert wird, wobei basierend auf der IMSI mittels von in einer SIM-Benutzerdatenbank abgespeicherten Informationen der logischen IP-Datenkanal des WLAN zu entsprechenden GSM-Daten für Signal- und Datenkanäle eines GSM-Netzwerkes benutzerspezifisch ergänzt wird, wobei mittels eines SIM-Gateway-Moduls zur Durchführung der Authentifizierung des IP-Nodes basierend auf den GSM-Daten die notwendigen SS7/MAP-Funktionen (Authentifikation und/oder Autorisation und/oder Konfigurationsinformationen) generiert werden, wobei das SIM-RADIUS-Modul mittels SIM-Benutzerdatenbank und SIM-Gateway-Moduls die Authentifizierung des mobilen IP-Nodes basierend auf der IMSI der SIM-Karte des mobilen Nodes bei einem HLR und/oder VLR eines GSM-Netzwerkes durchführt, und wobei bei erfolgreicher Authentifizierung ein Location Update sowie eine Service Autorisierung beim HLR und/oder VLR durchgeführt wird und der mobile IP-Node in einer Customer Database des Access Servers einen entsprechenden Eintrag erhält, wobei das WLAN zur Benutzung durch den mobilen IP-Node freigegeben wird. Bei erfolgreicher Authentifizierung kann als Ausführungsvariante zusätzlich zum Location Update beim HLR und/oder VLR eine Autorisierung des mobilen IP-Nodes durchgeführt werden, wobei beim HLR und/oder VLR ein entsprechendes Benutzerprofil basierend auf der IMSI heruntergelanden wird. D.h. die Service Autorisierung des Benutzers basiert auf der Abfrage des entsprechenden Benutzerprofils (Enduserprofil) beim HLR und/oder VLR. Das Genannte hat u.a. den Vorteil, dass ein automatisches Roaming zwischen unterschiedlichen und heterogenen WLANs und GSM-

Netzwerken möglich wird. Durch das Verbinden der WLAN-Technologie, insbesondere der IP-Netzwerke, mit der GSM-Technologie wird das Roaming des Benutzers möglich, ohne dass er sich um Anmeldung, Billing, Service Autorisation etc. bei den verschiedenen WLAN-Dienstanbietern bemühen müsste, d.h., dass der Benutzer den gleichen Komfort geniesst, wie er es von der Mobilfunktechnologie, wie z.B. GSM, gewohnt ist. Gleichzeitig ist es auf eine völlig neue Art möglich, die Vorteile der offenen IP-Welt (Zugang zum weltweiten Internet etc.) mit den Vorteilen des GSM-Standards (Sicherheit, Billing, Service Autorisation etc.) zu verbinden. Die Erfindung erlaubt auch ein Verfahren für ein Roaming in WLANs zu erzeugen, ohne dass bei jedem Access Server in entsprechendes Modul eingebaut werden müsste. Im Gegenteil kann die Infrastruktur (WLAN/GSM) durch die Verwendung von RADIUS unverändert übernommen werden.

In einer Ausführungsvariante wird für die Authentifizierung des mobilen IP-Nodes die auf der SIM-Karte des mobilen IP-Nodes gespeicherte IMSI nur bis zu einem oder mehreren der ersten Authentifikationsschritte benutzt und bei allen weiteren Authentifikationsschritten die IMSI durch eine generierte temporäre IMSI (TIMSI) ersetzt wird. Dies hat u.a. den Vorteil, dass die Sicherheit während der Authentifikation bzw. Autorisation erhöht werden kann.

In einer Ausführungsvariante wird die Authentifizierung des mobilen IP-Nodes mittels Extensible Authentication Protocol durchgeführt. Dies hat u.a. den Vorteil, dass in Kombination mit RADIUS ein vollständig Hardware und Hersteller (Vendor) unabhängiges Verfahren erzeugt wird. Insbesondere bietet EAP die notwendigen Sicherheitsmechanismen zur Durchführung der Authentifizierung.

In einer Ausführungsvariante wird der Datenstrom des mobilen IP-Nodes beim Zugriff auf das WLAN vom Access Point über einen Mobilfunknetzdienstanbieter geleitet. Dies hat u.a. den Vorteil, dass der Mobilfunknetzdienstanbieter vollständige Kontrolle über den Datenfluss hat. So kann er spezifisch Service Autorisationen vergeben, detailliertes Billing durchführen, Sicherheitsmechanismen einbauen und/oder personalisierte

Dienste anbieten. U.a. kann er damit die offene, schwierig zu kontrollierende IP-Welt mit beispielsweise dem Internet, mit den Vorteilen der GSM-Welt verbinden. Dies spielt gerade in neuerer Zeit z.B. bezüglich Haftungsfragen des Providers oder Dienstanbieters eine grosse Rolle.

In einer anderen Ausführungsvariante erteilt der Mobilfunknetzdienstanbieter basierend auf der Authentifizierung mittels der IMSI die entsprechende Service Autorisierung zur Benutzung unterschiedlicher Dienste und/oder führt das Billing der beanspruchten Leistung durch. Diese Ausführungsvariante hat u.a. die gleichen Vorteile wie die vorhergehende Ausführungsvariante.

In einer weiteren Ausführungsvariante ist die SIM-Benutzerdatenbank mit einer Sync-Datenbank zum Verändern oder Löschen von bestehenden Benutzerdatensätzen oder zum Einfügen neuer Benutzerdatensätze verbunden, wobei der Abgleich der Datenbanken periodisch durchgeführt wird und/oder durch Veränderungen der Sync-Datenbank und/oder durch Ausfall der SIM-Benutzerdatenbank ausgelöst wird. Dies hat den Vorteil, dass die Mobilfunknetzbetreiber zum Verändern oder Löschen von bestehenden Benutzerdatensätzen oder zum Einfügen neuer Benutzerdatensätze in gleicher Weise verfahren können wie bisher mit ihren Benutzerdatenbanken, dass heisst, ohne dass sie zusätzliche Systeme kaufen oder warten müssten.

In einer Ausführungsvariante werden mittels eines Clearing-Moduls für das Billing die Billing-Records der heterogenen WLANs mit den Benutzerdaten synchronisiert und basierend auf dem GSM-Standard TAP aufbereitet. Dies hat u.a. den Vorteil, dass Dienstabieter ohne Modifikation ihrer Software und/oder Hardware das vom GSM-Standard gewohnte Clearing- und Billingverfahren verwenden können. Insbesondere erfolgt damit auch die restliche Aufschlüsselung des IP-Datenstroms in einen GSM-Datenstrom.

An dieser Stelle soll festgehalten werden, dass sich die vorliegende Erfindung neben dem erfindungsgemässen Verfahren auch auf ein System zur Ausführung dieses Verfahrens bezieht.

Nachfolgend werden Ausführungsvarianten der vorliegenden Erfindung anhand von Beispielen beschrieben. Die Beispiele der Ausführungen werden durch folgende beigelegten Figuren illustriert:

Figur 1 zeigt ein Blockdiagramm, welches schematisch ein erfindungsgemässes Verfahren und eine System für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken illustriert, wobei mobile IP-Nodes 20 über eine kontaktbehaftete Schnittstelle mit einer SIM-Karte 201 und/oder ESIM (Electronic SIM) verbunden sind und mittels einer drahtlosen Verbindung 48 auf Access Points 21/22 des WLAN zugreifen. Ein Access Server 23 des WLAN authentifiziert den mobilen IP-Node 20 basierend auf einer auf der SIM-Karte 201 abgespeicherten IMSI bei einem HLR 37 und/oder VLR 37 eines GSM Mobilfunknetzes.

Figur 2 zeigt ein Blockdiagramm, welches schematisch ebenfalls ein erfindungsgemässes Verfahren und eine System für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken illustriert, wobei mobile IP-Nodes 20 über eine kontaktbehaftete Schnittstelle mit einer SIM-Karte 201 verbunden sind und mittels einer drahtlose Verbindung 48 auf ein WLAN zugreifen. Das WLAN ist über einen Access Server 23 mit einem GSM Mobilfunknetz, insbesondere einem HLR 37 und/oder VLR 37, einem GGSN (Gateway GPRS Support Node) 50 über ein GRX-Modul 51 (GRX: GPRS Roaming eXchange), einen Internet Service Provider 52 und einen Clearing Provider 53 für das Clearing der beanspruchten Leistungen über einen Clearing System Operator 54 mit dem entsprechenden Billing-System 55 des Internet Service Providers 52 verbunden. Die Referenznummern 60-64 sind bidirektionale Netzwerkverbindungen.

Figur 3 zeigt ein Blockdiagramm, welches schematisch ein Verfahren und eine System für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken illustriert, wobei die offene IP-Welt mittels dem erfindungsgemässen Verfahren und System über Schnittstellen der Authentifizierung 371 und Autorisierung 372 (SS7/MAP), Service Autorisierung 531 und Billing 532 mit der restriktiveren GSM-Welt verbunden sind.

Figur 4 zeigt ein Blockdiagramm, welches schematisch den Aufbau eines IEEE 802.1x Port-basierendes Authentifikationsverfahren illustriert, wobei der Supplicant oder Remote Access Client 20 über ein Authenticator oder Remote Access Server 21 bei einem Authentifikations-Server 23 authentifiziert wird, wobei das WLAN auf IEEE 802.11 basiert.

Figur 5 zeigt ein Blockdiagramm, welches schematisch eine mögliche Ausführungsvariante zur SIM-Authentifizierung mittels Extensible Authentification Protocol (EAP) illustriert, wobei ein GSM basiertes Challenge-Response Verfahren verwendet wird.

Figur 1 illustriert eine Architektur, die zur Realisierung der Erfindung verwendet werden kann. Figur 1 zeigt ein Blockdiagramm, welches schematisch ein erfindungsgemässes Verfahren und ein System für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken illustriert. In der Figur 1 bezieht sich das Bezugszeichen 20 auf einen mobile IP-Node, welcher über die notwendige Infrastruktur, einschliesslich Hardware- und Softwarekomponenten verfügt, um ein beschriebenes erfindungsgemässes Verfahren und/oder System zu realisieren. Unter mobile Nodes 20 sind u.a. alle möglichen sog. Customer Premise Equipment (CPE) zu verstehen, die zur Benutzung an verschiedenen Netzwerkstandorten und/oder verschiedenen Netzwerken vorgesehen sind. Diese umfassen beispielsweise sämtlich IP-fähigen Geräte wie z.B. PDAs, Mobilfunktelefone und Laptops. Die mobilen CPEs oder Nodes 20 besitzen ein oder mehrere verschiedene physikalische Netzwerkschnittstellen, die auch mehrere unterschiedliche Netzwerkstandards unterstützen können. Die physikalischen Netzwerkschnittstellen des mobilen Nodes können z.B. Schnittstellen zu WLAN (Wireless Local Area Network), Bluetooth, GSM (Global System for Mobile Communication), GPRS (Generalized Packet Radio Service), USSD (Unstructured Supplementary Services Data), UMTS (Universal Mobile Telecommunications System) und/oder Ethernet oder einem anderen Wired LAN (Local Area Network) etc. umfassen. Die Referenznummer 48 steht dementsprechend für die verschiedenen heterogenen Netzwerke, wie z.B. ein Bluetooth-Netzwerk, z.B. für Installationen in überdachten Örtlichkeiten, ein Mobilfunknetz mit GSM und/oder UMTS etc., ein Wireless LAN z.B. basierend

auf IEEE wireless 802.1x, aber auch einem Wired LAN, d.h. einem lokalen Festnetz, insbesondere auch dem PSTN (Public Switched Telephone Network) etc.. Prinzipiell ist zu sagen, dass das erfindungsgemässe Verfahren und/oder System nicht an einen spezifischen Netzwerkstandart gebunden ist, sofern die erfindungsgemässen Merkmale vorhanden sind, sondern können mit einem beliebigen LAN realisiert werden. Die Schnittstellen 202 des mobilen IP-Nodes können nicht nur packet-switched Schnittstellen, wie sie von Netzwerkprotokollen wie z.B. Ethernet oder Tokenring direkt benutzt werden, sondern auch circuit-switched Schnittstellen, die mittels Protokollen wie z.B. PPP (Point to Point Protocol), SLIP (Serial Line Internet Protocol) oder GPRS (Generalized Packet Radio Service) benutzt werden können, d.h. welche Schnittstellen z.B. keine Netzwerkadresse wie eine MAC- oder eine DLC-Adresse besitzen. Wie teilweise erwähnt, kann die Kommunikation über das LAN, beispielsweise mittels speziellen Kurzmeldungen, z.B. SMS (Short Message Services), EMS (Enhanced Message Services), über einen Signalisierungskanal, wie z.B. USSD (Unstructured Supplementary Services Data) oder andere Techniken, wie MExE (Mobile Execution Environment), GPRS (Generalized Packet Radio Service), WAP (Wireless Application Protocol) oder UMTS (Universal Mobile Telecommunications System) oder über IEEE wireless 802.1x oder einen anderen Nutzkanal erfolgen. Der mobile IP-Node 20 kann ein Mobile IP-Modul und/oder ein IPsec-Modul umfassen. Die Hauptaufgabe des Mobile IP besteht darin, den mobilen IP-Node 20 im IP-Netzwerk zu authentifizieren und die IP-Pakete, die den mobilen Node 20 als Zieladresse haben, entsprechend umzuleiten. Zu den weiteren Mobile IP Spezifikationen siehe z.B. auch IETF (Internet Engineering Task Force) RFC 2002, IEEE Comm. Vol. 35 No. 5 1997 etc. Mobile IP unterstützt insbesondere IPv6 und IPv4. Die Mobile IP Fähigkeiten können vorzugsweise mit den Sicherheitsmechanismen eines IPsec (IP security protocol)-Moduls kombiniert werden, um ein sicheres mobiles Datenmanagement im öffentlichen Internet zu garantieren. IPsec (IP security protocol) erzeugt paketweise oder socketweise Authentifikations-/Vertraulichkeitsmechanismen zwischen Netzwerkknoten, die beide IPsec benutzen. Eine der Flexibilitäten von IPsec liegt insbesondere darin, dass es sich paketweise aber auch für einzelne Sockets konfigurieren lässt. IPsec unterstützt IPvx, insbesondere IPv6 und IPv4. Für detailliertere IPsec-Spezifikationen siehe z.B. Pete Loshin: IP Security Architecture; Morgan

Kaufmann Publishers; 11/1999 oder A Technical Guide to IPsec; James S et al.; CRC Press, LLC; 12/2000 etc. Obwohl IPsec bei diesem Ausführungsbeispiel als Beispiel für die Verwendung von Sicherheitsprotokollen auf IP-Niveau beschrieben worden ist, sind alle möglichen anderen Sicherheitsprotokolle oder -mechanismen oder gar das Weglassen von Sicherheitsprotokollen erfindungsgemäss vorstellbar.

Weiter ist der mobile IP-Node 20 über eine kontaktbehaftete Schnittstelle mit einer SIM-Karte 201 (SIM: Subscriber Identity Module) verbunden, auf welcher eine IMSI (International Mobile Subscriber Identifier) eines Benutzers von GSM-Netzwerken abgespeichert ist. Das SIM kann sowohl hardwaremässig als SIM-Karte und/oder softwaremässig als elektronische SIM realisiert sein. Zur Authentifizierung fordert der mobiler IP-Node 20 über eine drahtlose Schnittstelle 202 innerhalb einer Basic Service Area eines WLANs bei einem Access Point 21/22 Zugriff auf das WLAN. Wie bereits beschrieben, können die verschiedenen WLANs unterschiedlicher Hot Spots heterogene Netzwerkstandards und -protokolle umfassen, wie z.B. WLAN basierend auf dem IEEE wireless 802.1x, Bluetooth etc.. Die Basic Service Area des WLAN umfasst ein oder mehrere einem Access Server 23 zugeordnete Access Points 21/22. Der mobile IP-Node 20 übermittelt auf einen Request des Access Servers 23 eine auf der SIM-Karte 201 des mobilen IP-Nodes 20 gespeicherte IMSI an den Access Server 23. Die IMSI des mobilen IP-Nodes 20 wird mittels eines SIM-RADIUS-Moduls 30 gespeichert. Basierend auf der IMSI wird mittels von in einer SIM-Benutzerdatenbank 34 abgespeicherten Informationen der logischen IP-Datenkanal des WLAN zu entsprechenden GSM-Daten für Signal- und Datenkanäle eines GSM-Netzwerkes benutzerspezifisch ergänzt. Das GSM System umfasst Datenkanäle, die sog. Traffic Channels, und Kontrolsignalkanäle, sog. Signaling Channels. Die Traffic Channeles (z.B. GPRS, GSM-Voice, GSM-Daten etc.) sind für Benutzerdaten reserviert, während die Signaling Channels (z.B. MAP, SS7 etc.) für Netzwerk-Managment, Kontrollfunktionen etc. verwendet werden. Die logischen Kanäle sind über die Schnittstelle nicht alle gleichzeitig benutzbar, sondern anhand der GSM-Spezifikationen nur in bestimmten Kombinationen. Mittels eines SIM-Gateway-Moduls 32 werden zur Durchführung der Authentifizierung des IP-Nodes basierend auf den GSM-Daten die notwendigen SS7/MAP-Funktionen

(Authentifikation und/oder Autorisation und/oder Konfigurationsinformationen) generiert, wobei das SIM-RADIUS-Moduls 30 mittels SIM-Benutzerdatenbank 34 und SIM-Gateway-Moduls 32 die Authentifizierung des mobilen IP-Nodes basierend auf der IMSI der SIM-Karte 201 des mobilen Nodes 20 bei einem HLR 37 (Home Location Register) und/oder VLR 37 (Visitor Location Register) eines GSM-Netzwerkes durchführt. Bei erfolgreicher Authentifizierung kann als Ausführungsvariante zusätzlich zum Location Update beim HLR (37) und/oder VLR 37 eine Autorisierung des mobilen IP-Nodes 20 durchgeführt werden, wobei beim HLR 37 und/oder VLR 37 ein entsprechendes Benutzerprofil basierend auf der IMSI heruntergelanden wird. Es ist auch vorstellbar, dass für die Authentifizierung des mobilen IP-Nodes 20 nur bei einem oder mehreren der ersten Authentifikationsschritte die auf der SIM-Karte des mobilen IP-Nodes 20 gespeicherte IMSI benutzt wird und bei allen weiteren Authentifikationsschritten die IMSI durch eine generierte temporäre IMSI (TIMSI) ersetzt wird. Für das Billing können die Billing-Records der heterogenen WLANs mit den Benutzerdaten (IMSI/TIMSI) mittels eines Clearing-Modul 533 synchronisiert werden und entsprechend aufbereitet werden, so dass diese z.B. im GSM-Standard TAP (Transferred Account Procedure), insbesondere im TAP-3 Standard, von Mobilfunkdienstanbietern ohne Anpassung ihres Billingsystems für die Weiterverwendung an ihre Kunden übernommen werden können. Die Transferred Account Procedure ist ein Protokoll für die Abrechnung zwischen verschiedenen Netzbetreibern, wobei die Version 3 (TAP-3) auch das Billing von Value Added Services in GPRS beherrscht.

Wie in Figur 5 illustriert, kann die Authentifizierung des mobilen IP-Nodes 20 z.B. mittels Extensible Authentication Protocol durchgeführt werden. Für das EAP-basierende Verfahren zur Authentifizierung eines Benutzers und zur Vergabe von Sessions Keys an den Benutzer mittels des GSM Subscriber Identity Modul (SIM) kann z.B. folgendes Challenge-Response Verfahren verwendet werden. Dem Authentifikationsalgorithmus der SIM-Karte wird als Challenge (Frage) eine 128-bit Zufallszahl (RAND) gegeben. Auf der SIM-Karte läuft dann ein für den jeweiligen Operator spezifischer, vertraulicher Algorithmus, der als Input die Zufallszahl RAND und einen geheimen, auf der SIM-Karte gespeicherten Schlüssel Ki erhält und daraus eine 32-bit Antwort (SRES) und ein 64-bit Schlüssel Kc generiert. Kc dient zur Verschlüsselung des

Datentransfers über drahtlose Schnittstellen (GSM Technical Specification GSM 03.20 (ETS 300 534): "Digital cellular telecommunication system (Phase 2); Security related network functions", European Telecommunications Standards Institute, August 1997). Zur Authentifizierung werden mehrere RAND Challenge zum Generieren von mehreren 64-bit Kc Schlüsseln verwendet. Diese Kc-Schlüssel werden zu einem längeren Session Key kombiniert. Figur 4 zeigt schematisch den Aufbau zwischen dem mobilen IP-Node 20, dem Access Point 21 und dem Access Server 23 in einem IEEE 802.1x Port-basierenden Authentifikationsverfahren, wobei der mobile IP-Node 20 (Remote Access Client / Supplicant) über den Access Point 21 (Authenticator) beim Access Server 23 (Authentifikations-Server) authentifiziert wird. Das WLAN basiert in diesem Ausführungsbeispiel auf IEEE 802.11. Um die GSM-Authentifikation durchzuführen, fungiert das SIM-Gateway-Modul 32 als Gateway zwischen Internet Authentification Service (IAS) Server Netzwerk und der GSM Authentifikationsinfrastruktur, d.h. dem Access Point 21/22 bzw. dem Access Server 23 und dem HLR 37 bzw. dem VLR 37. Zu Beginn der EAP/SIM Authentifizierung verlangt der Access Server 23 mit einem ersten EAP-Request 1 durch den Access Point 21/22 vom mobilen IP-Node 20 u.a. die International Mobile Subscriber Identity (IMSI) des Benutzer. Diese wird vom mobilen IP-Node mittels EAP-Response 2 an den Access Point 21/22 übermittelt. Mit der IMSI erhält der Access Server 23 auf eine Triplet-Anfrage vom entsprechenden HLR 37 bzw. VLR 37 bezeichnet, n GSM Triplets. Basierend auf den Triplets kann der Access Server 23 ein Message Authentification Code für n*RAND und eine Lebensdauer für den Schlüssel (zusammen MAC_RAND) sowie einen Session Schlüssel erhalten. In einem 3. EAP-Schritt 3 (Figur 5) schickt der Access Server 23 dann z.B. einen EAP-Request vom Typ 18 (SIM) an den mobilen IP-Node 20 und erhält die entsprechende EAP-Response 4. EAP-Datenpackete vom Typ SIM haben zusätzlich ein spezielles Subtyp-Feld. Der erste EAP-Request/SIM ist vom Untertype 1 (Start). Dieses Packet enthält die Liste der EAP/SIM Protokoll Versions-Nummern, die durch den Access Server 23 unterstützt werden. Der EAP-Response/SIM (Start) 4 (Figur 5) des mobilen IP-Nodes 20 enthält die vom mobilen IP-Node 20 ausgewählte Versionsnummer. Der mobile IP-Node 20 muss eine der im EAP-Request angegebenen Versionsnummern auswählen. Der EAP-Response/SIM (Start) des mobilen IP-Nodes 20 enthält ebenfalls einen Lebensdauervorschlag für den

Schlüssel (Key) und eine Zufallsnummer NONCE_MT, die durch den mobilen IP-Node generiert wurde. Alle folgenden EAP-Requests enthalten alle die gleiche Version wie das EAP-Response/SIM (Start) Datenpacket des mobilen IP-Nodes 20. Wie erwähnt, besitzt diese Ausführungsvariante um die GSM-Authentifikation durchzuführen ein SIM-Gateway-Modul 32, das als Gateway zwischen dem Access Server 23 und dem HLR 37 bzw. dem VLR 37 fungiert. Nach Erhalt der EAP-Response/SIM erhält der Access Server 23 ein n GSM Triplet vom HLR/VLR 37 des GSM-Netzwerkes. Aus den Triplets berechnet der Access Server 23 MAC_RAND und den Session Key K. Die Berechnung der kryptographischen Werte des SIM-generierten Session Key K und der Message Authentification Codes MAC-Rand und MAC_SRES könne beispielsweise dem Dokument "HMAC: Keyed-Hashing for Message Authentification" von H. Krawczyk, M. Bellar und R. Canetti (RFC2104, Feb. 1997) entnommen werden. Der nächste EAP-Request 5 (Figur 5) des Access Servers 23 ist vom Typ SIM und Subtyp Challenge. Der Request 5 enthält die RAND Challenges, die vom Access Server 23 beschlossene Lebensdauer des Schlüssels, ein Message Authentication Code für die Challenges und die Lebenszeit (MAC_RAND). Nach Erhalt des EAP-Request/SIM (Challenge) 5 läuft der GSM-Authentifikationsalgorithmus 6 auf der SIM-Karte und berechnet eine Kopie von MAC_RAND. Der mobile IP-Node 20 kontrolliert, dass der berechnete Wert von MAC_RAND gleich dem erhaltenen Wert von MAC_RAND ist. Ergibt sich keine Übereinstimmung der beiden Werte, bricht der mobile IP-Node 20 das Authentifikationsverfahren ab und schickt keine von der SIM-Karte berechneten Authentifikationswerte an das Netzwerk. Da der Wert RAND zusammen mit dem Message Authentifikations-Code MAC_RAND erhalten wird, kann der mobile IP-Node 20 sicherstellen, dass RAND neu ist und vom GSM-Netzwerk generiert wurde. Sind alle Überprüfungen richtig gewesen, schickt der mobile IP-Node 20 ein EAP-Response/SIM (Challenge) 7, der als Antwort MAC_SRES des mobilen IP-Nodes 20 enthält. Der Access Server 23 überprüft, dass MAC_RES korrekt ist und schickt schliesslich ein EAP-Success Datenpacket 8 (Figur 5), welches dem mobilen IP-Node 20 anzeigt, dass die Authentifizierung erfolgreich war. Der Access Server 23 kann zusätzlich den erhaltenen Session Key mit der Authentifizierungs-Meldung (EAP-Success) an den Access Point 21/22 schicken. Bei erfolgreicher Authentifizierung wird ein Location Update beim HLR 37 und/oder VLR 37 durchgeführt und der mobile IP-Node 20 erhält

in einer Customer Database des Access Servers einen entsprechenden Eintrag, wobei das WLAN zur Benutzung durch den mobilen IP-Node 20 freigegeben wird. Wie erwähnt, hat dies u.a. den Vorteil, dass ein automatisches Roaming zwischen unterschiedlichen und heterogenen WLANs möglich wird. Durch das Verbinden der WLAN-Technologie, insbesondere der IP-Netzwerke, mit der GSM-Technologie wird das Roaming des Benutzers möglich, ohne dass er sich um Anmeldung, Billing, Service Autorisation etc. bei den verschiedenen WLAN-Dienstanbietern bemühen müsste, d.h. dass der Benutzer den gleichen Komfort geniesst, wie er es von der Mobilfunktechnologie, wie z.B. GSM, gewohnt ist. Gleichzeitig ist es auf eine völlig neue Art möglich, die Vorteile der offenen IP-Welt (Zugang zum weltweiten Internet etc.) mit den Vorteilen (Sicherheit, Billing, Service Autorisation etc.) zu verbinden. Die Erfindung erlaubt auch ein Verfahren für ein Roaming in WLANs zu erzeugen, ohne dass bei jedem Access Server ein entsprechendes Modul eingebaut werden müsste. Im Gegenteil kann die Infrastruktur (WLAN/GSM) durch die Verwendung von RADIUS unverändert übernommen werden. Die Erfindung ermöglicht dadurch ein automatisches Roaming zwischen heterogenen WLANs, GSM-, GPRS- und UMTS-Netzwerken.

Figur 3 zeigt in einem Blockdiagramm noch einmal schematisch ein erfindungsgemässes Verfahren und System, wie über die Schnittstellen der Authentifizierung 371 und Autorisierung 372 (SS7/MAP), Service Autorisierung 531 und Billing 532 die offene IP-Welt 57 mit der restriktiveren GSM-Welt 58 verbunden sind. Die Referenznummer 38 geben dabei unterschiedliche Mobilfunknetzdienstanbieter mit zugeordneten HLR/VLR 37 an. Als Ausführungsvariante ist es vorstellbar, dass der Datenstrom des mobilen IP-Nodes 20 beim Zugriff auf das WLAN vom Access Point 21/22 über den Mobilfunknetzdienstanbieter 38 geleitet wird. Dies erlaubt dem Mobilfunknetzdienstanbieter 38 basierend auf der Authentifizierung mittels der IMSI benutzerspezifische Service Autorisierung zur Benutzung unterschiedlicher Dienste zu erteilen und/oder benutzerspezifisches Billing der beanspruchten Leistung durchzuführen. Zur Service Autorisierung wird nach der Authentifikation des Benutzers neben den Location Update beim HLR/VLR 37 ein Benutzerprofil (Enduserprofil) heruntergeladen, aus welchem die

entsprechenden Angaben zur Service Autorisierung eines Benutzers entnommen werden können. Basierend auf dem Benutzerprofil werden im mobilen IP-Node 20 die entsprechenden Autorisierungsflags zur Freigabe oder Verweigerung bestimmter Dienste gesetzt. Die Servicefreigabe könnte prinzipiell auch z.B. mittels einem Modul 214 direkt beim Access Point 21/22 oder, falls der Datenstrom umgeleitet wird, beim Mobilfunknetzdienstanbieter 38 vorgenommen werden.

Es bleibt zu erwähnen, dass in einem erweiterten Ausführungsbeispiel zum oben genannten Ausführungsbeispiel die SIM-Benutzerdatenbank 34 mit einem Sync-Modul 35 und einer Sync-Datenbank 36 zum Verändern oder Löschen von bestehenden Benutzerdatensätzen oder zum Einfügen neuer Benutzerdatensätze verbunden ist, wobei der Abgleich der Datenbanken 34/36 periodisch durchgeführt wird und/oder durch Veränderungen der Sync-Datenbank 36 und/oder durch Ausfall der SIM-Benutzerdatenbank 34 ausgelöst wird. Das Sync-Modul 35 und die Sync-Datenbank 36 können wie die übrigen erfindungsgemässen Komponenten hardware- oder softwaremässig als eigenständige Netzwerkkomponenten, z.B. als eigenständiger IP-Node und/oder GSM-Komponente oder einer anderen Systemkomponente zugeordnet und/oder in eine andere Systemkomponente integriert realisiert sein. Mit dieser Ausführungsvariante können die Mobilfunknetzbetreiber 38 zum Verändern oder Löschen von bestehenden Benutzerdatensätzen oder zum Einfügen neuer Benutzerdatensätze in gleicher Weise verfahren, wie bisher mit ihren Benutzerdatenbanken, dass heisst, ohne dass sie zusätzliche System kaufen oder warten müssten.

Ansprüche

1. Verfahren für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken, bei welchem zur Authentifizierung ein mobiler IP-Node (20) über eine drahtlose Schnittstelle innerhalb einer Basic Service Area eines WLANs bei einem Access Point (21/22) Zugriff auf das WLAN fordert, wobei die Basic Service Area des WLAN ein oder mehrere einem Access Server (23) zugeordnete Access Points (21/22) umfasst, bei welchem der mobile IP-Node (20) auf einen Request des Access Servers (23) eine auf einer SIM-Karte (201) des mobilen IP-Nodes (20) gespeicherte IMSI an den Access Server (23) übermittelt und die IMSI des IP-Nodes (20) in einer Datenbank (31) eines SIM-RADIUS-Moduls (30) gespeichert wird, dadurch gekennzeichnet,

dass basierend auf der IMSI mittels von in einer SIM-Benutzerdatenbank (34) abgespeicherten Informationen der logischen IP-Datenkanal des WLAN zu entsprechenden GSM-Daten für Signal- und Datenkanäle eines GSM-Netzwerkes benutzerspezifisch ergänzt wird,

dass mittels eines SIM-Gateway-Moduls (32) zur Durchführung der Authentifizierung des IP-Nodes (20) basierend auf den GSM-Daten die notwendigen SS7/MAP-Funktionen generiert werden,

dass das SIM-RADIUS-Moduls (30) mittels SIM-Benutzerdatenbank (34) und SIM-Gateway-Moduls (32) die Authentifizierung des mobilen IP-Nodes (20) basierend auf der IMSI der SIM-Karte (201) des mobilen Nodes (20) bei einem HLR (37) und/oder VLR (37) eines GSM-Netzwerkes durchführt, und

dass bei erfolgreicher Authentifizierung ein Location Update beim HLR (37) und/oder VLR (37) durchgeführt wird und der mobile IP-Node (20) in einer Customer Database des Access Servers (23) einen entsprechenden Eintrag erhält, wobei das WLAN zur Benutzung durch den mobilen IP-Node (20) freigegeben wird.

2. Verfahren für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken nach Anspruch 1, dadurch gekennzeichnet, dass bei erfolgreicher Authentifizierung zusätzlich zum Location Update beim HLR (37) und/oder VLR (37) eine Autorisierung des mobilen IP-Nodes (20) durchgeführt wird, wobei beim HLR (37) und/oder VLR (37) ein entsprechendes Benutzerprofil basierend auf der IMSI heruntergelanden wird.

3. Verfahren für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, dass für die Authentifizierung des mobilen IP-Nodes (20) die auf der SIM-Karte des mobilen IP-Nodes (20) gespeicherte IMSI nur bis zu einem oder mehreren der ersten Authentifikationsschritte benutzt wird und bei allen weiteren Authentifikationsschritten die IMSI durch eine generierte temporäre IMSI ersetzt wird.

4. Verfahren für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass die Authentifizierung des mobilen IP-Nodes (20) mittels Extensible Authentication Protocol durchgeführt wird.

5. Verfahren für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass der Datenstrom des mobilen IP-Nodes (20) beim Zugriff auf das WLAN vom Access Point (21/22) über einen Mobilfunknetzdienstanbieter geleitet wird.

6. Verfahren für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken nach Anspruch 5, dadurch gekennzeichnet, dass der Mobilfunknetzdienstanbieter basierend auf der Authentifizierung mittels der IMSI die entsprechende Service Autorisierung zur Benutzung unterschiedlicher Dienste erteilt und/oder Billing der beanspruchten Leistung durchführt.

7. Verfahren für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass die SIM-Benutzerdatenbank (34) mit einem Sync-Modul (35) und einer Sync-Datenbank (36) zum Verändern oder Löschen von bestehenden Benutzerdatensätzen oder zum Einfügen neuer Benutzerdatensätze verbunden ist, wobei der Abgleich der Datenbanken (34/36) periodisch durchgeführt wird und/oder durch Veränderungen der Sync-Datenbank (36) und/oder durch Ausfall der SIM-Benutzerdatenbank (34) ausgelöst wird.

8. Verfahren für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass mittels eines Clearing-Moduls 533 für das Billing die Billing-Records der heterogenen WLANs mit den Benutzerdaten synchronisiert und basierend auf dem GSM-Standard TAP aufbereitet werden.

9. System für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken, welches System mindestens ein WLAN mit jeweils einer Basic Service Area umfasst, welche Basic Service Area eines WLANs einen oder mehrere einem Access Server (23) zugeordnete Access Points (21/22) umfasst, welche Access Points (21/22) eine drahtlose Schnittstelle (211) zum Kommunizieren mit mobilen IP-Nodes (20) umfassen und welche mobilen IP-Nodes (20) eine SIM-Karte (201) zum Speichern einer IMSI umfassen, dadurch gekennzeichnet,

dass der Access Server (23) ein SIM-RADIUS-Moduls (30) mit einer Datenbank (31) zum Speichern der IMSI umfasst, wobei basierend auf der IMSI mittels von in einer SIM-Benutzerdatenbank (34) abgespeicherten Informationen der logischen IP-Datenkanal des WLAN zu GSM-Daten für Signal- und Datenkanäle eines GSM-Netzwerkes benutzerspezifisch ergänzt wird,

dass das System eine SIM-Gateway-Modul (32) umfasst, mittels welchem zur Durchführung der Authentifizierung des mobilen IP-Nodes (20)

basierend auf den GSM-Daten die notwendigen SS7/MAP-Funktionen generierbar sind, und

dass der Access Server (23) eine Customer Database umfasst, in welche authentifizierte Benutzer des WLANS mittels dem SIM-RADIUS-Modul (30) eintragbar sind, wobei bei der Eintragung ein Location Update der IMSI des mobilen IP-Nodes (20) beim HLR (37) und/oder VLR (37) durchgeführt wird.

10. System für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken nach Anspruch 9, dadurch gekennzeichnet, dass bei erfolgreicher Authentifizierung zusätzlich zum Location Update mittels eines Benutzerprofils des HLR (37) und/oder VLR (37) eine Autorisierung des mobilen IP-Nodes (20) durchführbar ist.

11. System für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken nach einem der Ansprüche 9 oder 10, dadurch gekennzeichnet, dass für die Authentifizierung des mobilen IP-Nodes (20) bei mindestens einem der Authentifikationsschritte die IMSI durch eine mittles einem Modul generierte temporäre IMSI ersetztbar ist.

12. System für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken nach nach einem der Ansprüche 9 oder 11, dadurch gekennzeichnet, dass die Authentifizierung des mobilen IP-Nodes (20) mittels Extensible Authentication Protocol durchführbar ist.

13. System für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken nach einem der Ansprüche 9 oder 12, dadurch gekennzeichnet, dass das System ein Mobilfunknetzanbieter umfasst, über welchen der Datenstrom des mobilen IP-Nodes (20) beim Zugriff auf das WLAN vom Access Point (21/22) umleitbar ist.

14. System für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken nach Anspruch 13, dadurch gekennzeichnet, dass der Mobilfunknetzdienstanbieter ein Autorisierungs-

Modul umfasst, das basierend auf der Authentifizierung mittels der IMSI die entsprechende Service Autorisierung zur Benutzung unterschiedlicher Dienste erteilt, und/oder ein Clearing System (53) umfasst, das das Billing der beanspruchten Leistung durchführt.

15. System für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken nach einem der Ansprüche 9 bis 14, dadurch gekennzeichnet, dass das System eine Sync-Modul (35) mit einer Sync-Datenbank (36) umfasst, mittels welcher die SIM-Benutzerdatenbank (34) zum Verändern oder Löschen von bestehenden Benutzerdatensätzen oder zum Einfügen neuer Benutzerdatensätze verbunden ist, wobei der Abgleich der Datenbanken periodisch durchgeführt wird und/oder durch Veränderungen der Sync-Datenbank (36) und/oder durch Ausfall der SIM-Benutzerdatenbank (34) ausgelöst wird.

16. System für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken nach einem der Ansprüche 9 bis 15, dadurch gekennzeichnet, dass mittels eines Clearing-Moduls 533 für das Billing die Billing-Records der heterogenen WLANs mit den Benutzerdaten synchronisierbar sind und basierend auf dem GSM-Standard TAP aufbereitbar sind.

Zusammenfassung

Die Erfindung betrifft ein Verfahren für automatisches Roaming zwischen heterogenen WLANs und/oder GSM/GPRS/UMTS-Netzwerken, bei welchem zur Authentifizierung ein mobiler IP-Node (20) bei einem Access Point (21/22) Zugriff auf das WLAN fordert, bei welchem der mobile IP-Node (20) auf einen Request des Access Servers (23) eine auf einer SIM-Karte (201) des mobilen IP-Nodes (20) gespeicherte IMSI an den Access Server (23) übermittelt und bei welchem basierend auf der IMSI mittels von in einer SIM-Benutzerdatenbank (34) abgespeicherten Informationen der logischen IP-Datenkanal des WLAN zu entsprechenden GSM-Daten für Signal- und Datenkanäle eines GSM-Netzwerkes benutzerspezifisch ergänzt wird und die Authentifizierung des IP-Nodes (20) bei einem HLR (37) und/oder VLR (37) eines GSM-Netzwerkes durchgeführt wird.

(Figur 1)

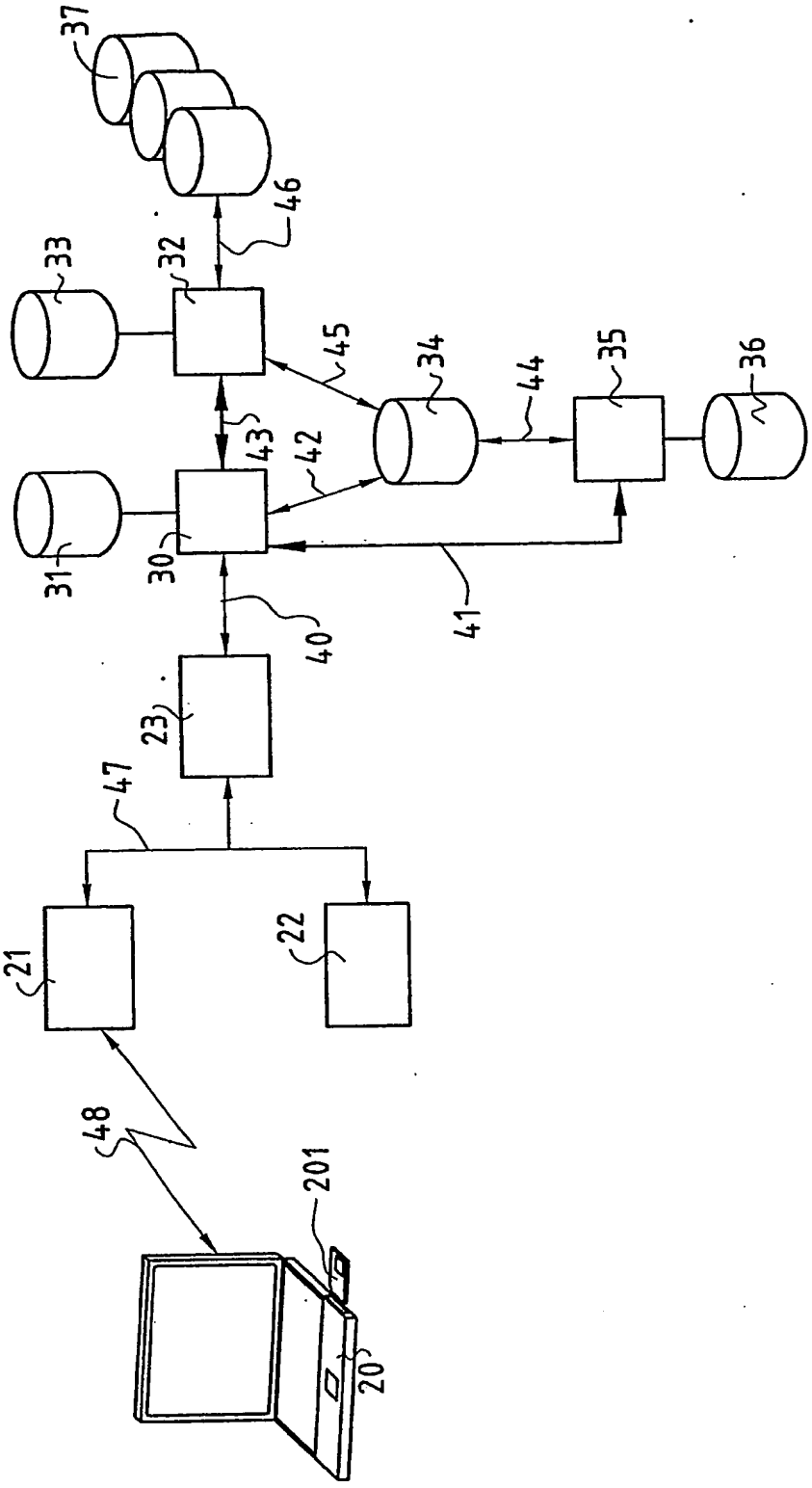

FIG. 1

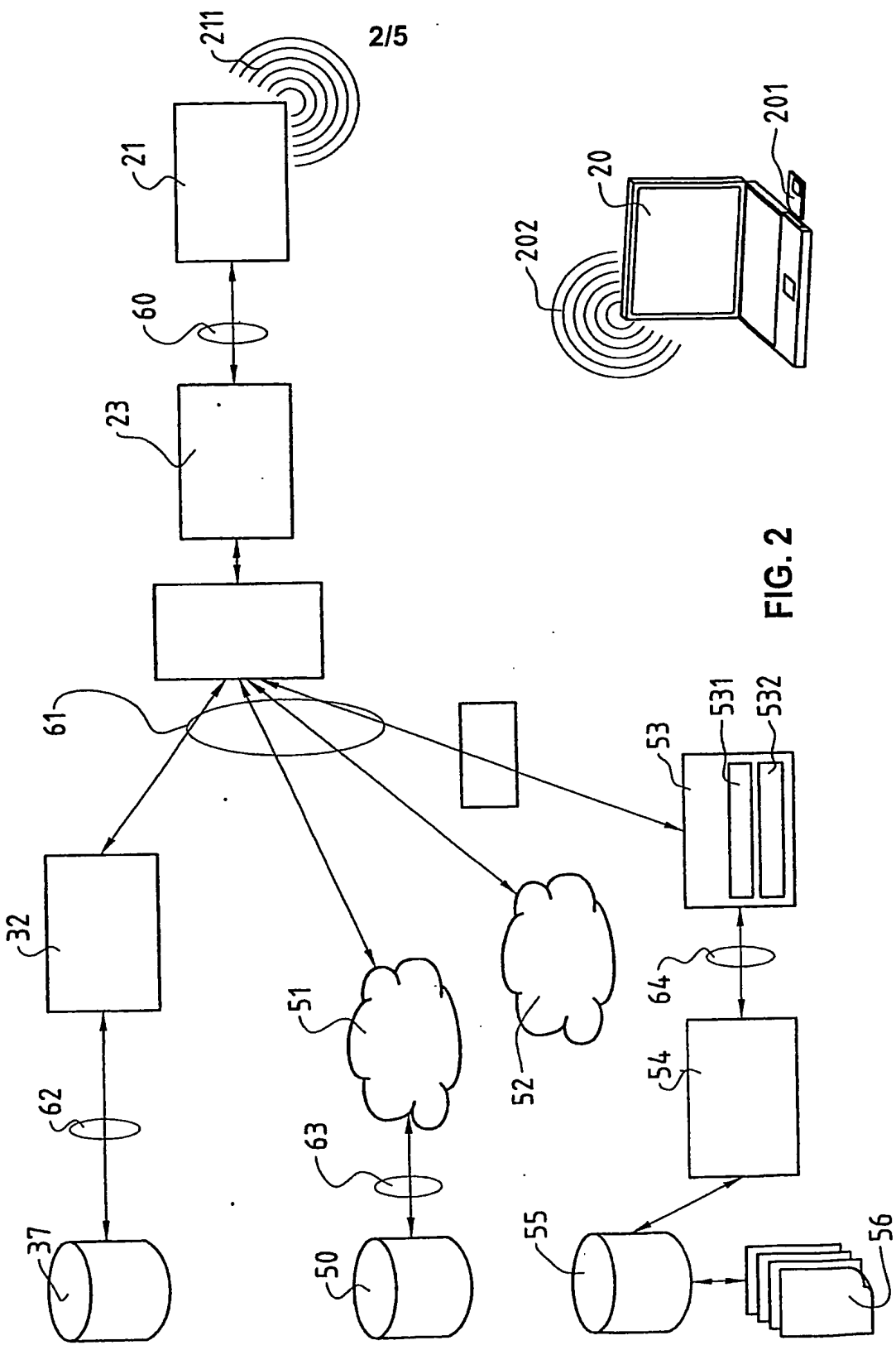

FIG. 2

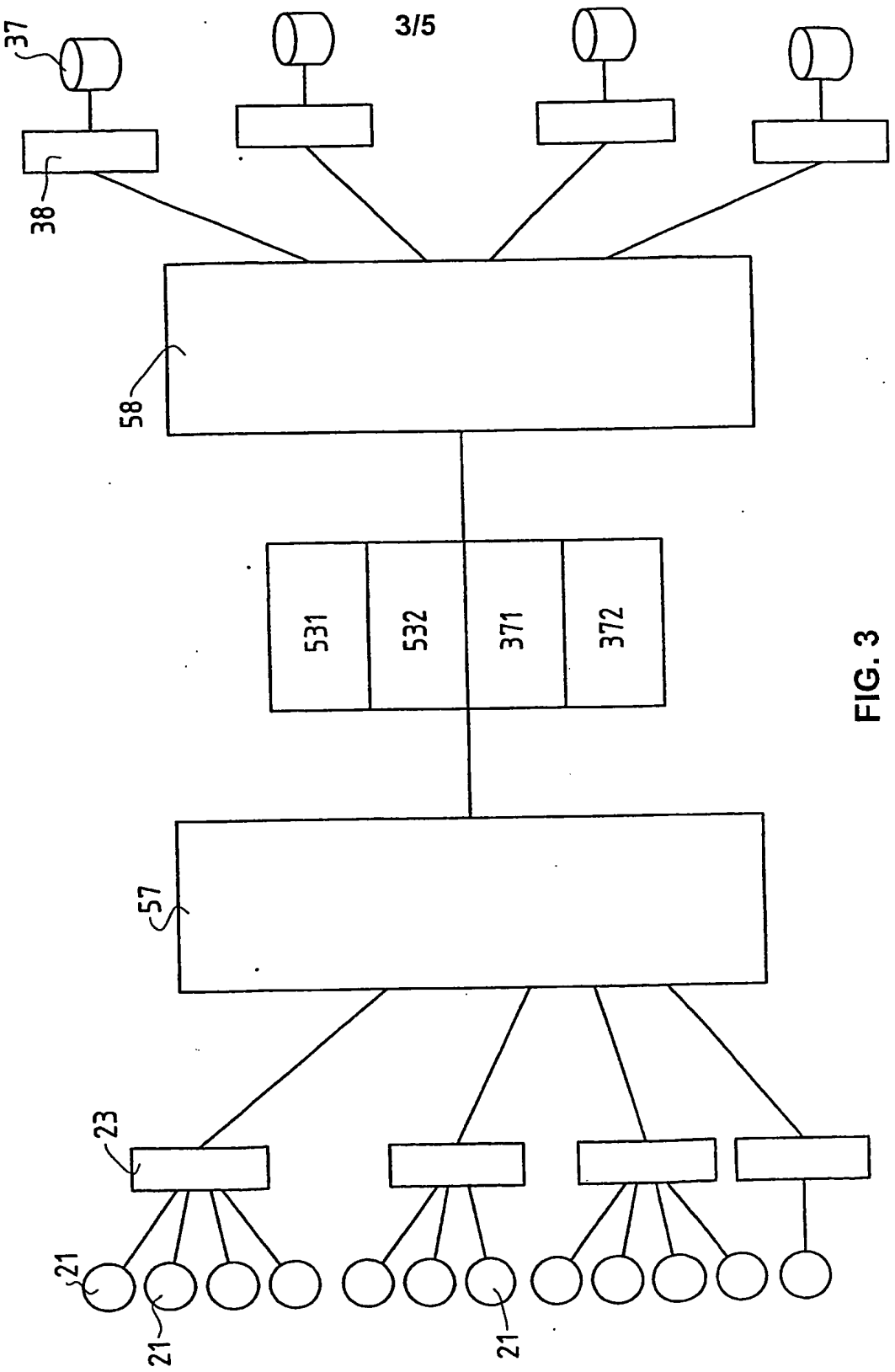

FIG. 3

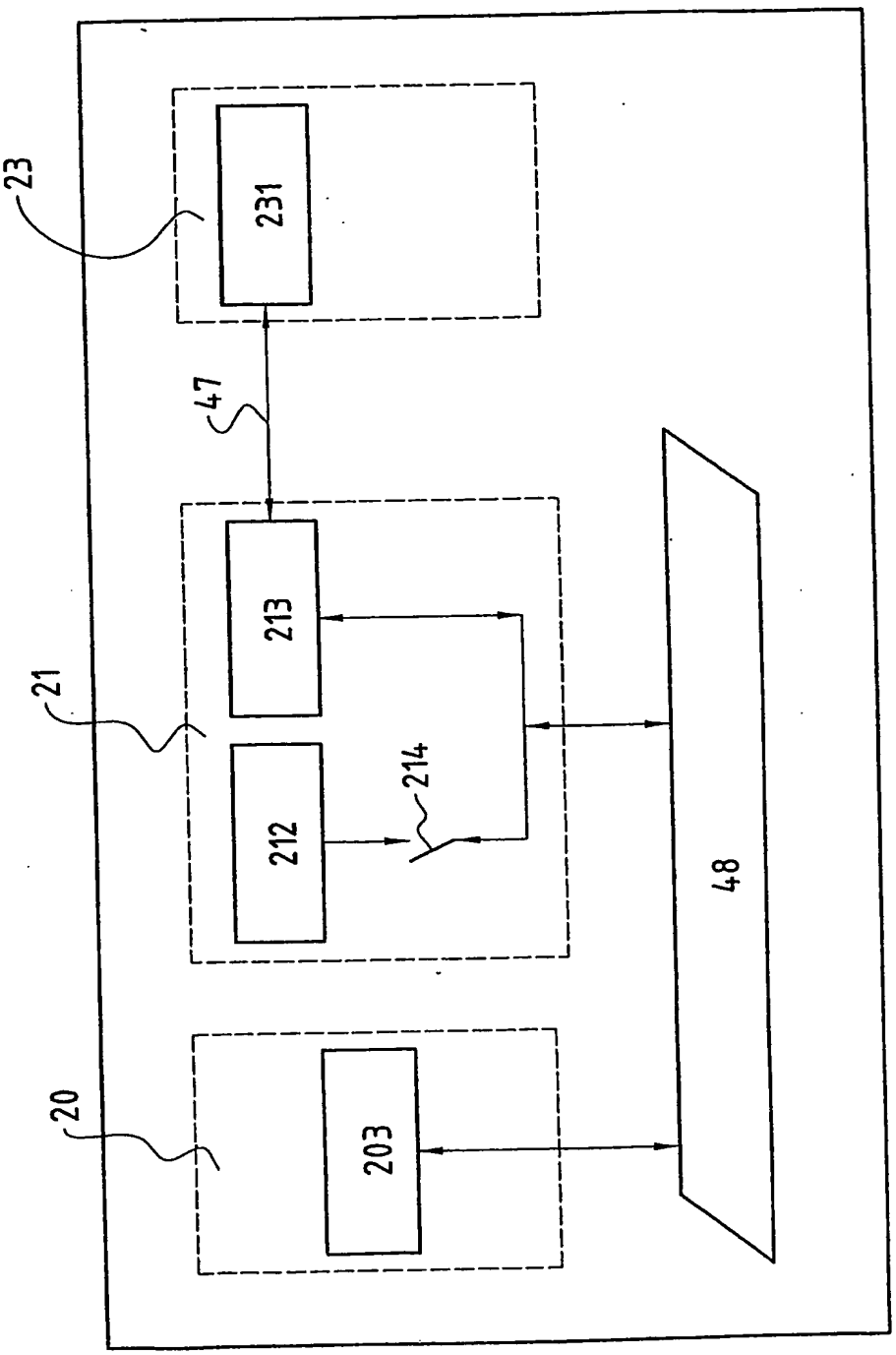

FIG. 4

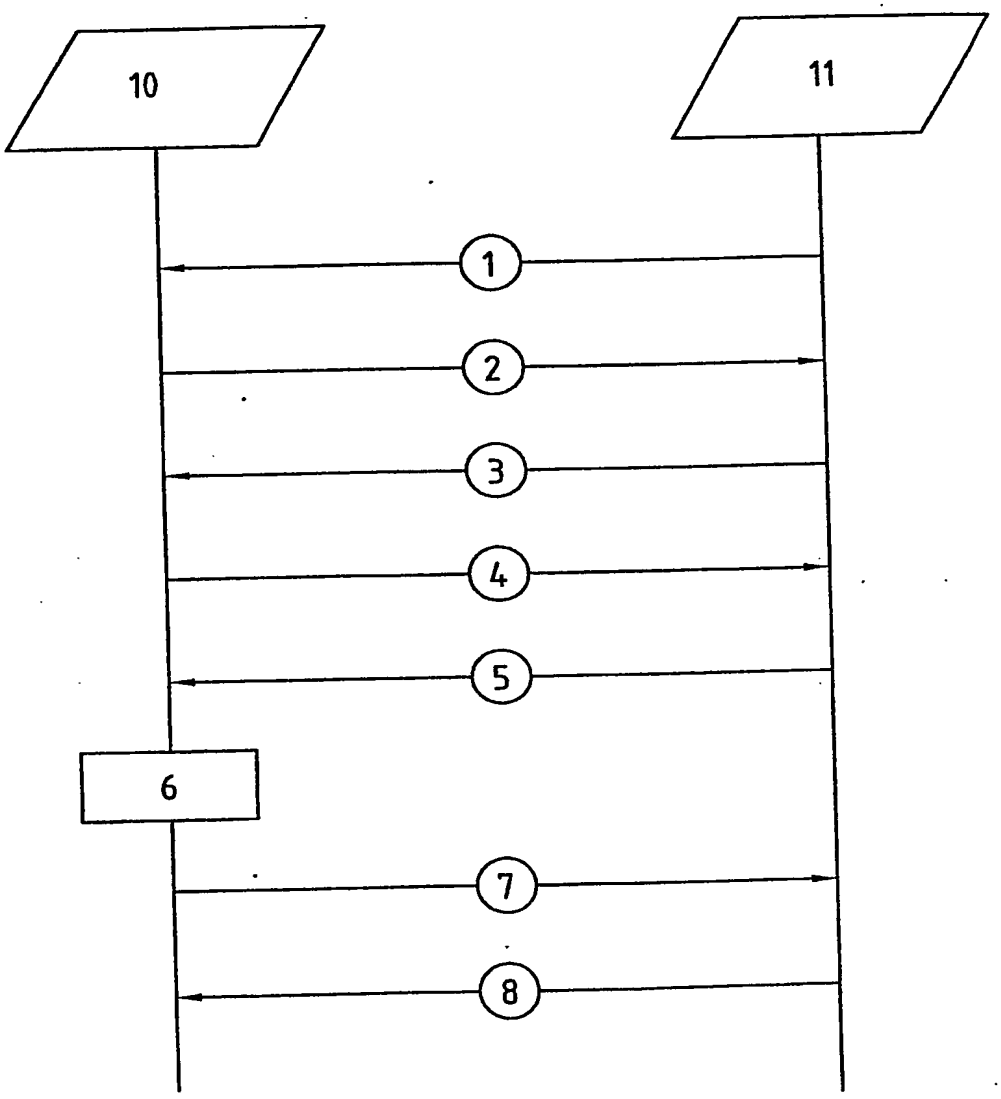

FIG. 5